REMARKS

1.   Summary of the Office Action

In the Office Action mailed May 30, 2006, the Examiner rejected claims 50-53 under 35 U.S.C. § 112, second paragraph, as failing to set forth the subject matter which Applicant regards as the invention. The Examiner rejected claims 1, 13, and 37 under 35 U.S.C. §102(b) as being anticipated by or, in the alternative, under 35 U.S.C. § 103(a) as being obvious over Charles P. Pfleeger, "Security in Computing," ISBN 013374866, 1996 (hereinafter "Pfleeger") as illustrated in U.S. Patent No. 6,141,755 (hereinafter "Dowd et al."). The Examiner rejected claims 1-8, 12-21, 24, 26, 31-32, 34, 36-38, 43, and 46-49 under 35 U.S.C. §102(e) as being anticipated by or, in the alternative, under 35 U.S.C. § 103(a) as being obvious over U.S. Patent No. 6,484,261 (hereinafter "Wiegel") as illustrated in Dowd et al. The Examiner rejected claims 9-11, 27, 33, 35, 42, and 44-45 under 35 U.S.C. §103(a) as being unpatentable over Wiegel in view of Official Notice. The Examiner rejected claims 50-53 under 35 U.S.C. § 103(a) as being obvious over Pfleeger as illustrated in Dowd et al. in view of Department of Defense, "Trusted Computer System Evaluation Criteria," Dec. 1985 (hereinafter "TCSEC"), and U.S. Patent No. 6,430,561 (hereinafter "Austel et al."). The Examiner also rejected claims 50-53 under 35 U.S.C. § 103(a) as being obvious over the combination of Wiegel, Dowd et al., TCSEC, and Austel et al. The Examiner objected to the drawings for not clearly disclosing the limitations found in the previously amended claim language and the specification.

2.   Amendments and Pending Claims

Applicant has amended claims 1, 13, 37, and 38, cancelled claims 50-53, and added new claims 54-56. Presently pending in this application are claims 1-21, 24, 26-28, 30-38, 42-45, and 54-56, of which claims 1, 13, 37, 38, and 56 are independent.

Applicant has amended the drawings. In particular, Applicant has amended Figure 2 to include the elements labeled 18 and 19 and the arrow connecting elements labeled 14 and 18. Support for the amendment to Figure 2 is located in the specification at page 6, lines 8-13.

Applicant has amended the specification by replacing the new paragraph added by the amendment filed March 7, 2006 (i.e., the new paragraph added after the paragraph that ends on page 9, line 19) with an amended paragraph. Support for this amendment is located in amended Figure 2 and in the specification at page 5, lines 3-6, and page 6, lines 8-13.

3. Payment of Fees

A fee of $200.00 is required for a new independent claim. Please charge this fee and any additional fees required under 37 C.F.R. §§ 1.16-1.21 or credit any overpayment of fees to Deposit Account No. 210765.

4. Response to Examiner's Claim Rejections

a. Rejections under 35 U.S.C. § 112, second paragraph

The Examiner rejected claims 50-53 under 35 U.S.C. § 112, second paragraph, as failing to set forth the subject matter which Applicant regards as the invention. In particular, the Examiner indicated the claim language is not clear as to how the trustworthiness measure differs from the criticality measure since both measures seem to be concerned with an assessment of a potential attack by the service components. Claims 50-53 have been cancelled. Thus, the rejection of claims 50-53 is moot. Even so, Applicant has amended independent claims 1, 13, 37, and 38 to include subject matter previously recited in claims 50-53. Applicant believes the amendments to claims 1, 13, 37, and 38 clearly distinguish the trustworthiness measure from the criticality measure such that a rejection of claims 1, 13, 37, and 38 under 35 U.S.C. § 112, second paragraph, is not proper.

b. **Rejections under 35 U.S.C. §§ 102 and 103**

The Examiner rejected claims 1, 13, and 37 under 35 U.S.C. § 102(b) as being anticipated by Plfeeger or, in the alternative, under 35 U.S.C. § 103(a) as being obvious over the combination of Pfleeger and Dowd et al. The Examiner rejected claims 1-8, 12-21, 24, 26, 31-32, 34, 36-38, 43, and 46-49 under 35 U.S.C. § 102(e) as being anticipated by Wiegel or, in the alternative, under 35 U.S.C. § 103(a) as being obvious over the combination of Wiegel and Dowd et al.

Applicant has amended independent claims 1, 13, 37, and 38 to include elements recited in cancelled claims 50-53 and to further distinguish the trustworthiness measure and criticality measure elements. The Examiner rejected claims 50-53 under: (i) 35 U.S.C. § 103(a) as being obvious over the combination of Pfleeger, Dowd et al., TCSEC, and Austel et al., and (ii) under 35 U.S.C. § 103(a) as being obvious over the combination of Wiegel, Dowd et al., TCSEC, and Austel et al.

According to M.P.E.P. § 2142, "[t]o reach a proper determination under 35 U.S.C. 103, the examiner must step backward in time and into the shoes worn by the hypothetical 'person of ordinary skill in the art' when the invention was unknown and just before it was made. In view of all factual information, the examiner must then make a determination whether the claimed invention 'as a whole' would have been obvious at that time to that person. Knowledge of applicant's disclosure must be put aside in reaching this determination, yet kept in mind in order to determine the 'differences,' conduct the search and evaluate the 'subject matter as a whole' of the invention. The tendency to resort to 'hindsight' based upon applicant's disclosure is often difficult to avoid due to the very nature of the examination process. However, impermissible

hindsight must be avoided and the legal conclusion must be reached on the basis of facts gleaned from the prior art."

As amended, independent claims 1, 13, 37, and 38 clearly distinguish over the combination of Pfleeger, Dowd et al., TCSEC, and Austel et al. and over the combination of Wiegel, Dowd et al., TCSEC, and Austel et al., because the combination of Pfleeger, Dowd et al., TCSEC, and Austel et al. and the combination of Wiegel, Dowd et al., TCSEC, and Austel et al., respectively, fail to disclose of suggest all of the limitations of any of these claims.

In particular, the combination of Pfleeger, Dowd et al., TCSEC, and Austel et al. and the combination of Wiegel, Dowd et al., TCSEC, and Austel et al. both fail to disclose or suggest: (i) for each (service or application) component, using the trustworthiness and criticality measures assigned to the (service or application) component so as to determine one or more of the processing nodes onto which the (service or application) component should be programmed, wherein the trustworthiness measure for each (service or application) component represents an assessment of a potential threat the (service or application) component poses to other objects, and wherein the criticality measure for each (service or application) component represents a measure of concern for what the other objects may do to the (service or application) component, as recited in claims 1, 13, and 37, or (ii), wherein for each application component, the trustworthiness and criticality measures assigned to the application component are used to determine one or more processing nodes onto which the application component should be loaded, wherein the trustworthiness measure for each application component represents an assessment of a potential threat the application component poses to other objects, and wherein the criticality measure for each application component represents a measure of concern for what the other objects may do to the application component, as recited in claim 38.

In rejecting claims 50-53, the Examiner indicated that Pfleeger and Wiegel do not teach using the trustworthiness and criticality measures of each service component to select the at least a respective one of the processing nodes onto which each service component should be programmed. Further, the Examiner stated "TCSEC does not explicitly teach considering trustworthiness measure and a respective criticality measure levels in selecting processing nodes onto which each service component should be programmed. However, the limitation is implicit." (Office Action of May 30, 2006, page 14, lines 15-17).

Applicant respectfully disagrees that the limitation of "using the trustworthiness and criticality measures of each service component to select at least a respective one of the processing nodes onto which each service component should be programmed" is implicit. At best, TCSEC teaches trusted computer system evaluation *criteria* that classify systems into four broad hierarchical divisions of enhanced security protection *to provide a basis for the evaluation of effectiveness of security controls built into automatic data processing system products* by (i) providing users with a yardstick with which to assess the degree of trust that can be placed in computer systems for the secure processing of classified or other sensitive information, (ii) providing guidance to manufacturers as to what to build into their new, widely-available trusted commercial products in order to satisfy trust requirements for sensitive applications, and (iii) providing a basis for specifying requirements in acquisition specifications. (TCSEC, page 6, emphasis added).

Assuming that the criteria disclosed in TCSEC teaches the trustworthiness and criticality measures recited in claims 1, 13, 37, and 38, which Applicant does not concede, TCSEC does not suggest nor does it not necessarily follow from the express teaching of TCSEC that the TCSEC criteria is used to determine one or more of the processing nodes onto which the service

- 23 -

component should be programmed. Rather, TCSEC merely teaches criteria for evaluating effectiveness of security controls built into automatic data processing system products.

Impermissible hindsight based on the Applicant's disclosure (e.g., disclosure regarding the use of trustworthiness and criticality measures assigned to the service component so as to determine one or more of the processing nodes onto which the service component should be programmed) must be avoided and legal conclusions must be reached on the basis of facts gleaned from the prior art.

In support of the Examiner's allegation that the limitation of using the trustworthiness and criticality measures of each service component to select at least a respective one of the processing nodes onto which each service component should be programmed is implicit, the Examiner indicated that Austel et al. teaches special measures (e.g., mandatory access controls) that have been devised to deal with non trusted software and that it would have been obvious to one of ordinary skill in the art at the time of Applicant's invention to select nodes with appropriate functionalities to complement the level of trustworthiness and criticality of respective service components that would be programmed into the node given the benefit of integrity, reliability, and availability, and the Examiner cited to Austel et al. col. 1 and 2.

At best, however, this section of Austel et al. teaches that (i) a first requirement of many security systems is preventing unauthorized disclosure of information, (ii) classes of mechanisms include discretionary access controls and mandatory access controls, (iii) mandatory access controls have been developed to deal with the Trojan horse problems of discretionary access controls, and (iv) the distinguishing feature of mandatory access controls is that the system manager or security officer may constrain the owner of an object in determining who may have access rights to that object. This section of Austel et al., as well as the rest of Austel et al., does

- 24 -

not teach or suggest: for each service component, using the trustworthiness and criticality measures assigned to the service component so as to determine one or more of the processing nodes onto which the service component should be programmed, wherein the trustworthiness measure for each service component represents an assessment of a potential threat the service component poses to other objects, and wherein the criticality measure for each service component represents a measure of concern for what the other objects may do to the service component.

Further, Dowd et al. fails to make up for the deficiencies of Pfleeger, Wiegel, TCSEC, and Austel et al. Although Dowd et al. is directed to an apparatus for high-speed circuit switched networks deployed between an external circuit switched network and an internal circuit switched network for preventing unauthorized communications between the external and internal circuit switched networks while permitting authorized communications between them, Dowd et al., alone or in combination with Pfleeger, TCSEC, and Austel et al. or Wiegel, TCSEC, and Austel et al., fails to teach or suggest: for each service component, using the trustworthiness and criticality measures assigned to the service component so as to determine one or more of the processing nodes onto which the service component should be programmed, wherein the trustworthiness measure for each service component represents an assessment of a potential threat the service component poses to other objects, and wherein the criticality measure for each service component represents a measure of concern for what the other objects may do to the service component. (See, e.g., Dowd et al., col. 5, lines 25-31).

Applicant submits that claims 1, 13, 37, and 38 are allowable because the combination of Pfleeger, Dowd et al., TCSEC, and Austel et al. and the combination of Wiegel, Dowd et al., TCSEC, and Austel et al., both fail to disclose or suggest all of the limitations of claims 1, 13,

- 25 -

37, and 38. Further, without conceding the assertions made by the Examiner regarding dependent claims 2-12, 14-21, 24, 26-28, 30-36, and 42-45, Applicant submits that dependent claims 2-12, 14-21, 24, 26-28, 30-36, 42-45, and 54-55 are allowable for at least the reason that they depend from one of allowable claims 1, 13, or 38.

5. Independent Claim 56

Applicant has added new independent claim 56. Support for claim 56, as well as new claims 54-55, may be found at originally filed claims 1 and 40, and in the specification at page 5, lines 15-17, page 6, lines 7-18, page 12, lines 19-21, and page 28, line 19, to page 29, line 8. Applicant submits that the prior art of record does not teach or suggest all of the elements recited in claim 56.

6. Conclusion

For the foregoing reasons, Applicant submits that claims 1-21, 24, 26-28, 30-38, 42-45, and 54-56 are in condition for allowance. Therefore, Applicant respectfully requests favorable reconsideration and allowance of all of the pending claims.

Respectfully submitted,

**MCDONNELL BOEHNEN
HULBERT & BERGHOFF LLP**

Date: _August 13_ , 2006   By: _David L. Ciesielski_
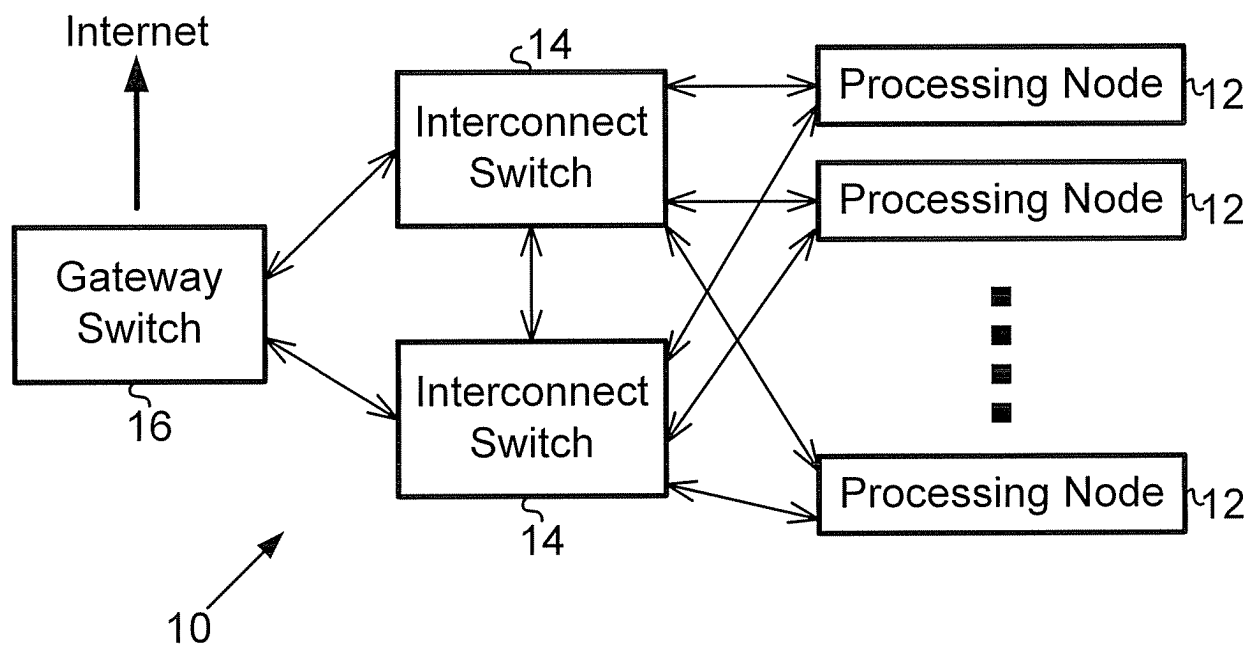
David L. Ciesielski
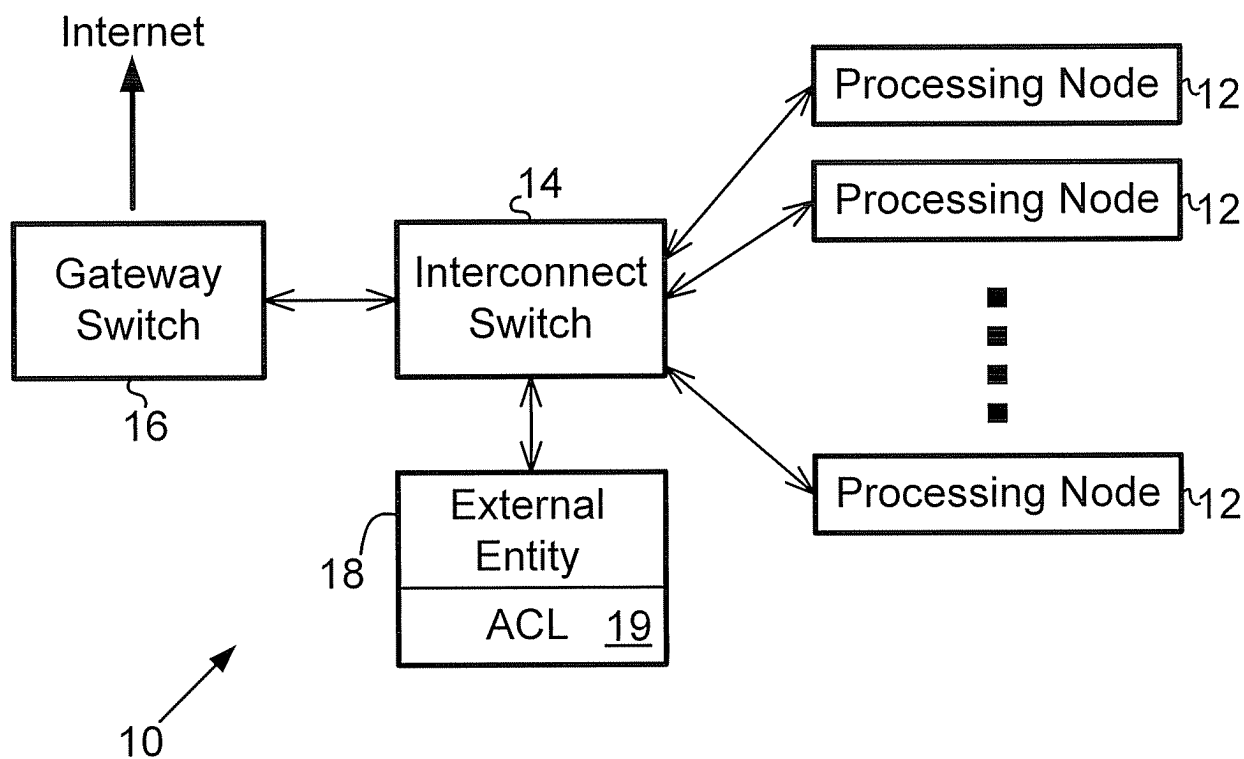Reg. No. 57,432

Replacement Drawing Sheet
Serial No. 09/941,326 – Inventors: Timothy Roscoe et al.
Title: Method and System for Communication Control in a Computing Environment

Fig. 1

Fig. 2